UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/761,040	01/20/2004	Marc Girault	5284-31	1201

7590 10/15/2008

COHEN, PONTANI, LIEBERMAN & PAVANE
Suite 1210
551 Fifth Avenue
New York, NY 10176

EXAMINER	
PERUNGAVOOR, VENKATANARAY	
ART UNIT	PAPER NUMBER
2432	
MAIL DATE	DELIVERY MODE
10/15/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/761,040	GIRAULT, MARC	
	Examiner	Art Unit	
	Venkat Perungavoor	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 August 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 8/14/2008 has been entered.

Response to Arguments

Applicant's arguments with respect to claims 1-32 have been considered but are moot in view of the new ground(s) of rejection.

Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent Publication 2002/0129247 to Jablon in view of US Patent 5867577 to Patarin and further in view of EP 0325238 to Yeda and further in view of US Patent 2001/0016910 to Tanimoto et al.(hereinafter Tanimoto).

Regarding Claim 1, 31, Jablon discloses the producing random number specific to transaction see Fig. 1 item 103; sending of parameter x, that is linked to random number r by a mathematical relationship see Fig. 1 item QA; calculating a parameter y whose input parameters are random number r specific to transaction and private key s see Fig. 1 item 105 & 107; sending the authentication value see item 108; verifying the authentication value using public key see item 127. But Jablon does not explicitly disclose a chip and an application conducting the said authentication. However, Patarin discloses the authentication between chip and application loaded onto a memory see Fig. 1. It would be obvious to one having ordinary skill in the art at the time of the invention to include chip and an application conducting the said authentication in the invention of Jablon in order to introduce the authentication on a carrier device as taught in Patarin see Col 1 Ln 10-21. But Jablon nor Patarin disclose the producing of pseudo-random number at application prior to a transaction, calculating a corresponding parameter x at the application prior to the transaction, and the parameter x being linked to pseudo-random number r by a mathematical relationship and storing of parameter x in memory of chip prior to the transaction. However, Yeda discloses the producing of pseudo-random number prior to a transaction see Fig. 1 item 14, calculating a corresponding parameter x at the application prior to the transaction, and the parameter x being linked to pseudo-random number r by a mathematical relationship see Fig. 1 item 12 and storing of parameter x in memory of chip prior to the transaction see Page 3 Ln 55-57. It would be obvious to one having ordinary skill in the art at the time of the

invention to include the using of parameter r and calculating of value x prior to the transaction in order to other end to easily verify the value x for authentication as taught in Yeda see Fig. 1 item 54. But Jablon nor Patarin nor Yeda disclose the generator being located within the chip. However, Tanimoto discloses random number generator located within a chip see Fig. 2 item "Random Number Generator". It would be obvious to one having ordinary skill in the art at the time of the invention to include a random number generator on a chip in the invention of Jablon in order to perform security operations with the processor at the other end as taught in Tanimoto see Fig. 2 item "Security Logic".

Regarding Claim 2 , Jablon does not disclose the mixing of input parameters by a mixing function, changing the state from old state to new state and determining a series of bits to form whole or portions of random number. However, Patarin discloses the a mixing function see Col 3 Ln 5, changing the state from old state to new state see Col 4 Ln 40-53 and determining a series of bits to form whole or portions of random number see Col 3 Ln 46-55. It would be obvious to one having ordinary skill in the art at the time of the invention to include mixing of input parameters by a mixing function, changing the state from old state to new state and determining a series of bits to form whole or portions of random number in the invention of Jablon in order to individually varying with card as taught in Patatin see Col 3 Ln 10-11.

Regarding Claim 3, Jablon discloses the sharing of keys between two entities see Abstract.

Regarding Claim 4, Jablon discloses the set of G belonging gr see Par. 0058 & Par. 0082.

Regarding Claim 5, 30, Jablon discloses the set G belonging to Zn, where it is set of positive or null integers less than n and prime see Par. 0084 & Par. 0037.

Regarding Claim 6, 31, Jablon discloses the set G being based on elliptical curve see Par. 0125.

Regarding Claim 7-10, 12, Jablon discloses the arithmetical operation from a list of addition, subtraction, and left- and right shifts see Par. 0131 & Par. 0149.

Regarding Claim 11, 13-29, Jablon discloses the various configurations of gr = x y see Par. 0146-0163 & Par. 0087-0089.

Claims 32 is rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent Publication 2002/0129247 to Jablon in view of US Patent 5867577 to Patarin, further in view of US Patent 2003/0182554 to Gentry et al.(hereinafter Gentry) and further in view

of US Patent 2001/0016910 to Tanimoto et al.(hereinafter Tanimoto) and further in view of EP 0325238 to Yeda.

Regarding Claim 32, Jablon nor discloses the exclusive use of public parameters to verify the authentication results. However, Gentry disclose the use of public parameters exclusively to verify the authentication results see Fig. 5 item 516. It would be obvious to one having ordinary skill in the art at the time of the invention to include the exclusive use of public parameters to verify the authentication results in the invention of Jablon in order to have to be able to increase the number of processors added to the network as taught in Gentry see Fig. 6. Jablon nor Patarin disclose the producing of pseudo-random number at application prior to a transaction, calculating a corresponding parameter x at the application prior to the transaction, and the parameter x being linked to pseudo-random number r by a mathematical relationship and storing of parameter x in memory of chip prior to the transaction. However, Yeda discloses the producing of pseudo-random number at application prior to a transaction see Fig. 1 item 14, calculating a corresponding parameter x at the application prior to the transaction, and the parameter x being linked to pseudo-random number r by a mathematical relationship see Fig. 1 item 12 and storing of parameter x in memory of chip prior to the transaction see Page 3 Ln 55-57. It would be obvious to one having ordinary skill in the art at the time of the invention to include the using of parameter r and calculating of value x prior to the transaction in order to other end to easily verify the value x for authentication as taught in Yeda see Fig. 1 item 54. But Jablon nor Patarin nor Yeda

disclose the generator being located within the chip. However, Tanimoto discloses random number generator located within a chip see Fig. 2 item "Random Number Generator". It would be obvious to one having ordinary skill in the art at the time of the invention to include a random number generator on a chip in the invention of Jablon in order to perform security operations with the processor at the other end as taught in Tanimoto see Fig. 2 item "Security Logic".

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Venkat Perungavoor whose telephone number is (571)272-7213. The examiner can normally be reached on M-Fri 8:30-5.
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/V. P./
Examiner, Art Unit 2132
September 22, 2008

/Benjamin E Lanier/
Primary Examiner, Art Unit 2132